UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/403,689	10/22/1999	BERND KOWALSKI	2345/97	7576

26646 7590 04/29/2003

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER
STULBERGER, CAS P

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 04/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/403,689	KOWALSKI ET AL.	
	Examiner	Art Unit	
	Cas Stulberger	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-7 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-4 is/are rejected.

7)☒ Claim(s) 5-7 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 October 1999 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Objections

1. Claims 5-7 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claims. See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,425,103 to Shaw, and further in view of U.S. Patent No. 5,142,578 to Matyas et al.

In regards to claim 1, Shaw discloses the user key may be input to the present invention directly in binary form or any other suitable form (Shaw: Abstract). If the base key is longer than the user key then the user key is duplicated and the copies are appended to one another. For example, if the base key (KV) has a length of 160 bits, a user key (KS) having a length of 48 bits must be duplicated three times (n) (Shaw: column 7, lines 60-68). This meets the limitation of "a defined key length (x bits) and using an optionally variable parameter (IV) having a length of n * x bits, a Vernam key (KV) is generated by way of any symmetrical cipher (S)." Shaw however does not disclose "the secret key (KS) and the parameter (IV) are communicated from the sender

to the recipient via a secure channel separate from the message-transmission path or directly on the message-transmission path, secured by an asymmetrical method."

Matyas et al. discloses that public key systems are bases on dispensing with the secret key distribution channel, as long as the channel has a sufficient level of integrity (Matyas: column 2, lines 27-29). This meets the limitation of "the secret key (KS) and the parameter (IV) are communicated from the sender to the recipient via a secure channel separate from the message-transmission path or directly on the message-transmission path, secured by an asymmetrical method." Matyas also discloses the symmetric algorithm Data Encryption Algorithm (DEA) (Matyas: column 2, lines 66-68). To transfer the DEA key over the secure channel it is encrypted with the private key and then sent to the recipient where it is decrypted with the public key (Matyas: column 3, lines 1-27).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of key creation as disclosed by Shaw with the method of key distribution as disclosed by Matyas in order to improve the integrity of a key distribution process (Matyas: Abstract).

4. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,425,103 to Shaw, in view of U.S. Patent No. 5,142,578 to Matyas et al as applied to claim 1 above, and further in view of U.S. Patent No. 5,513,261 to Maher.

Shaw however does not disclose a PCMCIA or chipcard which stores the Vernam Key.

Maher discloses a PCMCIA card on which a user might have keys coded (column 1, lines 31-33). This meets the limitations of "the storage for the Vernam key are installed in a crypto-

module separate from the encryptor, in the form of a chipcard, a multifunctional PC interface adapter, or module (PCMCIA) and only the Vernam cipher operations are performed in the encryptor."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of key distribution and creation as disclosed by Shaw with the method of storing the key on the PCMCIA card as disclosed by Maher in order to preclude the discovery of the security parameters by unauthorized parties (Maher: Abstract).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (703) 305-8034. The examiner can normally be reached on Monday - Friday, 8:30A.M. - 5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications, (703) 746-7240 for drafts, and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CS

CS
April 25, 2003

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100